JOSE LUIS RODRIGUEZ ALVAREZ (1 de 1)
Presidente
Fecha Firma: 23/02/2026
HASH: d315d9d6e4a6cfd91a7fd23c0ab51032

Resolución reclamación art. 24 LTAIBG

Número y fecha de resolución: indicados al margen.

Número de expediente: 2067/2025; 2108/2025 (acumulados)

Reclamante: [redacted]

Organismo: AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

Sentido de la resolución: Estimatoria.

Palabras clave: brecha de seguridad, protección de datos, autoridad de control, art. 33.1 RGPD, arts. 14.1.e) y g) LTAIBG.

R CTBG
Número: 2026-0198 Fecha: 23/02/2026

I. ANTECEDENTES

1. Según se desprende de la documentación obrante en el expediente, el 24 de julio de 2025 el reclamante solicitó a la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), al amparo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno [1] (en adelante, LTAIBG), la siguiente información:

   «El pasado 2 de abril de 2024, la Agencia Española de Protección de Datos me envió un escrito que iba dirigido a una empresa de la cual yo me desvinculé en octubre de 2019 (...). En ese escrito había diez anexos donde figuraban nombre, apellidos, nº de DNI y firmas manuscritas de los integrantes de la empresa. Esto resulta un fallo de seguridad en el envío de la comunicación y la difusión de datos personales a un tercero.

[1] https://www.boe.es/buscar/doc.php?id=BOE-A-2013-12887

Por tanto, quiero que se me facilite el documento público donde la AEPD comunica el error o la brecha de seguridad que hizo que se produjera ese error."

"1. Cualquier registro interno de la AEPD relativo a dicho incidente (...).

2. Actas, comunicaciones internas o informes técnicos o jurídicos del Delegado de Protección de Datos o de cualquier órgano de la AEPD donde se evalúe, informe o documente el envío indebido de documentación personal a un tercero»

Con fecha 22 de agosto de 2025, aportó copia de un escrito presentado ante la AEPD, con fecha 2 de abril de 2024, en el que comunicaba dicho incidente.

2. Mediante resolución de 23 de septiembre de 2025 la AEPD se concede parcialmente el acceso a la información manifestando lo siguiente:

«(...)4. De conformidad con lo establecido en el artículo 33 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, RGPD); se informa de que la AEPD, como responsable del tratamiento ha procedido a comunicar la violación de seguridad de los datos personales, de conformidad con lo dispuesto en el artículo 33 del RGPD.

5. La brecha de datos personales ha quedado debidamente documentada en la comunicación efectuada por el Delegado de Protección de Datos de la AEPD a la División de Innovación Tecnológica, unidad encargada de evaluar el riesgo y determinar las medidas que deben adoptarse.

6. El artículo 34.1 del RGPD obliga a comunicar las brechas de datos personales a los interesados solo cuando estas entrañen un alto riesgo para los derechos y libertades de las personas físicas.

Por tanto, dado que los datos de carácter personal contenidos en el escrito recibido por el solicitante eran meramente identificativos de personas físicas (nombre, apellidos, DNI y firma manuscrita) incluidos en un procedimiento, en el que el solicitante ostentaba la condición de interesado; la AEPD, como responsable de dicho tratamiento, ha determinado que no resulta aplicable lo dispuesto en el artículo 34 del RGPD por no entrañar un alto riesgo para los derechos y libertades de las personas físicas afectadas.

7. De esta manera queda facilitada la información pública cuyo acceso se solicita, sin que proceda el traslado al solicitante de la documentación cuya difusión afecta

R CTBG Número: 2026-0198 Fecha: 23/02/2026

a los sistemas de seguridad de la información de las entidades públicas y privadas en relación con el tratamiento de datos personales, razón por la cual la AEPD no la proporciona en aplicación de los límites al derecho de acceso recogidos en el artículo 14.1.e) y g) de la LTAIBG.

8. Efectivamente, la difusión de la información que recoge las causas de una violación de la seguridad de los datos personales que pudiera afectar a sus sistemas y medidas de seguridad y conforman la base sobre la que se han de llevar a cabo las actuaciones conducentes a la adopción de una decisión por parte de la autoridad de control, perjudicaría el desarrollo de las competencias en materia de protección de datos asignadas a la AEPD, como son la prevención, investigación y sanción de los ilícitos administrativos (art. 14.1.e LTAIBG) y las funciones administrativas de vigilancia, inspección y control (art. 14.1.g LTAIBG) que tiene asignadas, como recoge el considerando 87 del RGPD al señalar que una notificación de violación de la seguridad de los datos personales "puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento".

Por su parte, el Consejo de Transparencia y Buen Gobierno en su Resolución 103/2019, de 9 de mayo de 2019, recoge que la notificación a la autoridad de control de que se ha producido una violación de la seguridad de los datos de carácter personal se enmarca, "en las facultades de control para la protección de los datos de carácter personal y a los efectos de investigar las circunstancias en las que se ha producido esa quiebra en la seguridad debida respecto del tratamiento de los datos personales así como, en su caso, en la depuración de responsabilidades por incumplimiento de la normativa de protección de datos que pudiera derivarse de los hechos acontecidos

9. Por último y por lo expuesto en los Fundamentos anteriores, no procede atender la solicitud de una "certificación negativa en la que se indique que no se evaluó ni documentó internamente el error", toda vez que se ha informado de las actuaciones llevadas a cabo por la AEPD. Así mismo, se participa que el procedimiento de acceso a la información pública no tiene por objeto, en ningún caso, la emisión de certificaciones relativas a la información solicitada, lo que, en su caso, supondría su inadmisión por requerir reelaboración de la información (artículo 18.1.c de la LTAIBG). En este sentido, el concepto de reelaboración ha sido interpretado por el Consejo de Transparencia y Buen Gobierno en diversas resoluciones y en su criterio CI/007/2015, de tal manera que puede entenderse aplicable cuando la información que se solicita, perteneciendo al ámbito funcional de actuación del organismo o

R CTBG Número: 2026-0198 Fecha: 23/02/2026

entidad que recibe la solicitud, deba elaborarse expresamente para dar una respuesta».

3. Mediante escrito registrado el 25 de septiembre de 2025, el solicitante interpuso una reclamación ante el Consejo de Transparencia y Buen Gobierno (en adelante, el Consejo) en aplicación del artículo 24[2] LTAIBG en la que pone de manifiesto su disconformidad con la respuesta y expone que *«no solicito ningún documento que pueda afectar a cualquier control o investigación, estoy solicitando la documentación por la cual el delegado de protección de datos de la Agencia, comunicó la existencia de dicha brecha reconocida».*

   Ese mismo día, presenta escrito en el que manifiesta su conformidad con que se le entreguen *«los documentos por el cual el Delegado de Protección de Datos de la Agencia comunicó formalmente la existencia de la brecha de seguridad, pudiendo en su caso disociar los datos personales que contuviera»*, y otra instancia adjuntando distinta documentación relativa al asunto. A fin de identificar a qué resolución de acceso a la información pública se referían dichos escritos, este Consejo procedió a abrir el expediente número 2108/2025 y el 1 de octubre de 2025 se solicitó subsanación al efecto al interesado, quien el mismo día presenta escrito aclaratorio sobre que su intención era la de incorporar documentación al expediente número 2067/2025, exponiendo que *«los dos expedientes (2108/2025 y 2067/2025), que versan sobre la misma reclamación y la misma información pública solicitada».*

   El reclamante presenta otro escrito complementario el 26 de septiembre de 2025 en el que manifiesta que, en caso de que la información afecte a la seguridad, las funciones de inspección, control o investigación, o cualquier procedimiento disciplinario, acota el objeto de su reclamación a que se le facilite *«únicamente la parte del documento donde quede reflejada la fecha de dicha comunicación».* Expone que dicha información es esencial para determinar la cronología real de los hechos y no afecta a ninguno de los límites contemplados en el artículo 14 LTAIBG. Señala que la relevancia radica en «*conocer cómo reacciona la autoridad de control en materia de protección de datos cuando la brecha se produce siendo ella misma responsable del tratamiento*», y sostiene que la AEPD en procedimientos sancionadores contra terceros ha considerado circunstancias similares como agravantes.

   Posteriormente, el 28 de septiembre de 2025, el interesado presenta nuevo escrito en el que incide en la relevancia de conocer la fecha de comunicación de la brecha

[2] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a24

R CTBG Número: 2026-0198 Fecha: 23/02/2026

una vez que tuvo constancia de ella el 2 de abril de 2025 para «*saber si cumplió con el artículo 33 del RGPD*». A dicho escrito adjunta listado de los medios digitales que se han hecho eco de la noticia y «*conversación de whatsapp con un periodista que demuestra que la AEPD perdió el control del documento y no ha hecho nada hasta que he ejercido el derecho de supresión y los medios digitales se han hecho eco de la noticia».*

4. Con fecha 26 de septiembre de 2025, el Consejo trasladó la reclamación a la AEPD solicitando la remisión de la copia completa del expediente derivado de la solicitud de acceso a la información y el informe con las alegaciones que considere pertinentes. El 14 de octubre de 2025 tuvo entrada en este Consejo, junto al expediente, escrito de la Agencia en el que, reiterando lo expuesto en la resolución, se señala lo siguiente en relación con lo manifestado por el recurrente en la reclamación y los escritos complementarios:

   «La denegación de acceso a la información relativa a brechas de seguridad de datos personales es un criterio que ha sido mantenido por esta UIT y respaldado por el CTBG en diversas resoluciones (Resolución 103/2019 y 1964/2024).

   (…)

   Por tanto, la difusión de las circunstancias concretas en que tiene lugar la brecha podría afectar, no sólo a las funciones asociadas a la investigación de la propia violación de seguridad, sino que podrían quedar expuestos los sistemas y procedimientos internos para el análisis de las reclamaciones, su admisión a trámite y, en su caso, la tramitación de los procedimientos sancionadores que corresponden a la SGID.

   (…)

   - El artículo 16 de la LTAIBG contempla la concesión de acceso parcial "salvo que de ello resulte una información distorsionada o que carezca de sentido", lo que a juicio de esta UIT sucedería de proporcionarse tan solo la fecha de la notificación de la brecha por parte del DPD, sin el resto de información de contexto.

   - Debe tenerse en cuenta la particularidad de esta brecha, por cuanto el responsable del tratamiento y la autoridad de control coinciden, cabiendo la posibilidad de que existiera otra información de carácter interno, intercambiada entre unidades administrativas, que quedaría excluida del acceso, de conformidad con el artículo 18.1.b) de la LTAIBG.

R CTBG Número: 2026-0198 Fecha: 23/02/2026

- Así mismo, téngase en cuenta que no siempre es obligada la notificación a la autoridad de control, sino únicamente cuando las consecuencias de la brecha impliquen un posible alto riesgo para los derechos y libertades de las personas físicas afectadas. En el presente caso, no ha sido posible determinar la existencia de un alto riesgo para los derechos y libertades de las personas afectadas por la brecha, en particular, tanto por la obligación de confidencialidad a la que el recurrente está obligado, como por ser de su conocimiento previo los datos que le han sido revelados como consecuencia de la brecha. En este sentido, dada la coincidencia de obrar tanto en calidad de responsable como de Autoridad de Control, la anotación de cualquier brecha en el registro de brechas de esta Autoridad forma parte de la propia gestión interna de este organismo dado que el registro de brechas está siendo utilizado para la gestión, análisis, clasificación y documentación de cualquier brecha que pueda sobrevenir en los tratamientos de los que es responsable esta Agencia, con independencia del nivel de riesgo que pudiera derivarse como resultado de las mismas.

(...)

La cronología de los hechos es conocida: la brecha se produce el 2 de abril de 2024 (como queda acreditado en la resolución de acceso a la información pública que se recurre), cuando el recurrente recibe, por error, un requerimiento de aclaraciones no dirigido a él. Cabe recalcar que esta notificación se produce en el contexto de un expediente en el que el recurrente tiene la condición, asimismo, de reclamante por la vulneración de la normativa de protección de datos, y que la notificación trae causa de un escrito presentado por él mismo.

En cuanto a la relevancia pública que pueda tener la reacción de la autoridad de control cuando actúa como responsable, es importante distinguir con claridad las obligaciones de la AEPD como responsable del tratamiento de datos, de sus obligaciones como Autoridad de Control en este caso concreto:

Las violaciones de seguridad disfrutan de un régimen específico de publicidad, de conformidad con los artículos 33 y 34 del RGPD. El artículo 33 recoge los casos en que existe la obligación de notificar dicha violación a la autoridad de control a la vez que recoge la obligación del responsable de documentar cualquier violación de la seguridad de datos personales, mientras que en el artículo 34 prevé aquéllos en que se deberá comunicar a los interesados.

(...)

R CTBG Número: 2026-0198 Fecha: 23/02/2026

De este artículo [33 RGPD] *se puede concluir que no en todos los casos es obligatoria la notificación a la autoridad de control y cabe la posibilidad de que dicha notificación se produzca pasadas las 72 horas, como ocurre cuando es improbable que la brecha de datos personales constituya un riesgo para los derechos y libertades de las personas físicas afectadas, posibilidad que omite el recurrente. Por lo que la fecha de la notificación, a juicio de esta Agencia, no reviste la relevancia pública que el recurrente le otorga dado que, tal como ha quedado expuesto, quedaría totalmente descontextualizada sin el resto de información, en particular, los elementos de juicio por los que el responsable del tratamiento vino a valorar el riesgo inherente de la brecha para los afectados si no se tiene en cuenta la obligación de confidencialidad del recurrente y la circunstancia de que ya tenía conocimiento previo de los afectados.*

(...)

En la resolución reclamada, la AEPD (como responsable, no como autoridad de control) informa al solicitante de que, dado que los datos de carácter personal contenidos en el escrito recibido por el recurrente eran meramente identificativos de personas físicas (nombre, apellidos, DNI y firma manuscrita) y estaban incluidos en un procedimiento en el que, por ostentar la condición de interesado, no resultaba aplicable lo dispuesto en el artículo 34 del RGPD, dado que los datos no entrañaban un alto riesgo para los derechos y libertades de las personas físicas afectadas.

A mayor abundamiento, tras un análisis posterior de la brecha, esta AEPD ha confirmado que los diez nombres y apellidos, así como ocho de los DNI contenidos en la notificación ya eran conocidos por el recurrente, habiendo sido aportados por él mismo en un procedimiento anterior seguido por la SGID.

(...)

El recurrente asegura que los datos personales de terceras personas físicas, a los que tuvo acceso como resultado de la brecha estuvieron, "expuestos durante meses" en los siguientes términos, lo que considera relevante para su reclamación de acceso: "Ese mismo documento fue colgado en la sede electrónica de la AEPD, accesible públicamente mediante Código Seguro de Verificación (CSV)"

En respuesta a esta afirmación, la AEPD hace constar (aunque no es objeto de la reclamación ante el CTBG) que dicho documento nunca ha estado públicamente accesible en la sede electrónica

(...)

R CTBG Número: 2026-0198 Fecha: 23/02/2026

- La única persona con acceso al CSV que permitía obtener el documento electrónico en el que se contenían los datos personales afectados por la brecha era el recurrente. Por lo que la AEPD nunca ha perdido el control de dichos datos.

- Es importante destacar aquí que, al recibir estos datos de carácter personal, el recurrente se convierte en responsable de cualquier tratamiento ulterior de los mismos (independientemente de que dicho acceso se haya producido como consecuencia de una brecha) y que cualquier tratamiento de datos personales requiere de una causa de legitimación de las recogidas en el artículo 6 del RGPD.

- Como afirma el propio recurrente, y aporta documentación acreditativa, facilitó a terceros (mediante una conversación de WhatsApp) el código CSV y la fecha de la firma del documento recibido por error, dando así acceso a los datos personales objeto de la brecha, lo que supondría un tratamiento de datos personales que requeriría de una legitimación además del cumplimiento del resto de obligaciones exigibles en la normativa de protección de datos personales y del resto de normativas que le pudieran ser de aplicación.

(...)

En definitiva,

- La denegación de acceso a la información relativa a las notificaciones de brechas, reguladas en los artículos 33 y 34 del RGPD, de conformidad con los artículos 14.1 e) y g) es un criterio que ha sido aplicado por la AEPD a todas las solicitudes de acceso a esta información y que ha sido, ampliamente, respaldado por el CTBG.

- La AEPD, en su calidad de responsable, ha cumplido con las obligaciones recogidas en el RGPD, no teniendo más obligaciones de publicidad de las brechas que las estipuladas en estos artículos. Especialmente, cuando el recurrente no ostenta la condición de afectado por la brecha de datos de carácter personal.

- Del acceso al dato de la fecha de la notificación realizada por el DPD de la AEPD, a la unidad competente de la AEPD, sin el resto de información de contexto resultaría una información distorsionada y carente de sentido.

- El ahora recurrente alega un interés público que no puede reconducirse, a juicio de esta Agencia, a ninguna de las finalidades de la LTAIBG, en tanto en cuanto la AEPD, como autoridad de control, solo tiene la misión de recibir las notificaciones y, en su caso, iniciar las actuaciones administrativas de vigilancia, inspección y control que tiene asignadas y que podrían verse afectadas por la divulgación de dicha información.

R CTBG
Número: 2026-0198 Fecha: 23/02/2026

- En cuanto al posible interés público que pudiera haber en la existencia de la brecha reconocida ha quedado satisfecho con la divulgación en medios digitales efectuada por el propio recurrente, que aporta enlaces a diversos medios digitales que confirman que la brecha de datos personales, sufrida por la AEPD, como responsable del tratamiento, es ya de dominio público.

- La revelación de la información solicitada a terceros podría perjudicar posibles actuaciones de investigación por parte de la AEPD. La información solicitada podría estar relacionada con actuaciones de investigación, y su difusión a terceros podría perjudicar las actuaciones y diligencias a practicar por esta Agencia».

5. El 16 de octubre de 2025, se concedió audiencia al reclamante para que presentase las alegaciones que estimara pertinentes; recibiéndose escrito el mismo día en el que reitera su interés en conocer *«cómo actuó el organismo que se encarga del cumplimiento del RGPD cuando le afecta como responsable del tratamiento, sobre todo, la fecha en que se comunicó la brecha de seguridad reconocida».* Posteriormente, mediante escritos de 27 de octubre de 2025, 19 de noviembre de 2025 y 3 de diciembre de 2025, el reclamante presenta nueva documentación referente al incidente objeto de su solicitud y reitera su interés en que *«la información solicitada (especialmente la fecha de notificación) permitiría determinar si la AEPD cumplió sus obligaciones como responsable del tratamiento»*.

II. FUNDAMENTOS JURÍDICOS

1. De conformidad con lo dispuesto en el artículo 38.2.c) de la LTAIBG[3] y en el artículo 13.2.d) del Real Decreto 615/2024, de 2 de julio, por el que se aprueba el Estatuto del Consejo de Transparencia y Buen Gobierno, A.A.I.[4], el presidente de esta Autoridad Administrativa Independiente es competente para conocer de las reclamaciones que, en aplicación del artículo 24 de la LTAIBG[5], se presenten frente a las resoluciones expresas o presuntas recaídas en materia de acceso a la información.

2. La LTAIBG reconoce en su artículo 12[6] el derecho de todas las personas a acceder a la información pública, entendiendo por tal, según dispone en el artículo 13, «*los*

[3] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&p=20181206&tn=1#a38
[4] https://www.boe.es/eli/es/rd/2024/07/02/615
[5] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&p=20181206&tn=1#a24
[6] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a12

R CTBG Número: 2026-0198 Fecha: 23/02/2026

contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones».

De este modo, la LTAIBG delimita el ámbito material del derecho a partir de un concepto amplio de información, que abarca tanto documentos como contenidos específicos y se extiende a todo tipo de "*formato o soporte*". Al mismo tiempo, acota su alcance, exigiendo la concurrencia de dos requisitos que determinan la naturaleza "*pública*" de las informaciones: (a) que se encuentren "*en poder*" de alguno de los sujetos obligados, y (b) que hayan sido elaboradas u obtenidas "*en el ejercicio de sus funciones*".

Cuando se dan estos presupuestos, el órgano competente debe conceder el acceso a la información solicitada, salvo que justifique de manera clara y suficiente la concurrencia de una causa de inadmisión o la aplicación de un límite legal.

3. La presente reclamación trae causa de una solicitud, formulada en los términos que figuran en los antecedentes, en la que se pide el acceso a distinta información referida a una violación de la seguridad de los datos personales cometida por AEPD y denunciada por el solicitante.

   La AEPD dictó resolución en la que acuerda de conceder parcialmente el acceso, indicando que, de conformidad con establecido en el artículo 33 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), «*como responsable del tratamiento ha procedido a comunicar la violación de seguridad de los datos personales*», y que «[l]*a brecha de datos personales ha quedado debidamente documentada en la comunicación efectuada por el Delegado de Protección de Datos de la AEPD a la División de Innovación Tecnológica, unidad encargada de evaluar el riesgo y determinar las medidas que deben adoptarse*». Asimismo, informa que no se ha considerado aplicable lo dispuesto en el artículo 34 RGPD en relación con la comunicación de la brecha a los interesados porque los datos revelados eran meramente identificativos (nombre, apellidos, DNI y firma manuscrita) incluidos en un procedimiento en el que el destinatario ostentaba la condición de interesado y no se consideró que su revelación entrañase un alto riesgo para los derechos y libertades de las personas físicas.

   El resto de la información solicitada se deniega por considerar aplicables los límites de las letras e) y g) del artículo 14.1 LTAIBG —perjuicio para la prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios; y

R CTBG Número: 2026-0198 Fecha: 23/02/2026

perjuicio para las funciones administrativas de vigilancia, inspección y control de la AEPD—.

Una vez recibida la respuesta, el interesado acota el objeto de su solicitud en el escrito de reclamación ante el Consejo a «*la documentación por la cual el delegado de protección de datos de la Agencia, comunicó la existencia de dicha brecha*», o, subsidiariamente, a la fecha de esa comunicación, para finalmente circunscribir en el trámite de audiencia su pretensión a «*la fecha en que se comunicó la brecha de seguridad reconocida*» .

4. A requerimiento del Consejo, se ha aclarado por parte del interesado que las instancias que presenta el 25 de septiembre de 2025 y dan lugar a la apertura de dos expedientes (2067/2025 y 2108/2025), se refieren a la misma solicitud, por lo que resulta oportuna la acumulación de las dos reclamaciones interpuestas a fin de dar una única respuesta, en la medida en que se reúnen los requisitos que, para la acumulación, se establecen en el artículo 57 de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPAC) según cuyo tenor *«el órgano administrativo que inicie o tramite un procedimiento, cualquiera que haya sido, la forma de su iniciación, podrá disponer, de oficio o a instancia de parte, su acumulación a otros con los que guarde identidad sustancial o íntima conexión, siempre que sea el mismo órgano quien deba tramitar y resolver el procedimiento».*

5. Por otra parte, antes de entrar en el análisis de las cuestiones de fondo, conviene precisar que el objeto de este proceso no es la pretensión de acceder a toda la información enunciada en la solicitud inicial, sino la mucho más limitada, fruto de las acotaciones realizadas por el propio reclamante en el transcurso de este procedimiento, circunscribiéndola finalmente al dato relativo a «*la fecha en la que se comunicó la brecha de seguridad reconocida*».

   Acotado en estos términos el objeto de la reclamación, este Consejo ha de partir de que la información demandada obra en poder del órgano reclamado. A este respecto, no cabe desconocer que, aunque en sus alegaciones posteriores pone de manifiesto que «*no en todos los casos es obligatoria la notificación a la autoridad de control y cabe la posibilidad de que dicha notificación se produzca pasadas las 72 horas,»* en la resolución sobre el acceso indicó expresamente que «*la AEPD, como responsable del tratamiento ha procedido a comunicar la violación de seguridad de los datos personales, de conformidad con lo dispuesto en el artículo 33 del RGPD».*

R CTBG Número: 2026-0198 Fecha: 23/02/2026

6. Pues bien, es cierto que, tal y como destaca la AEPD, este Consejo ha considerado justificada la denegación del acceso a la información técnica (y a la referida al origen y las consecuencias de las brechas de seguridad) contenida en las comunicaciones que los responsables del tratamiento de datos personales deben realizar a la Autoridad de control en cumplimiento de la obligación impuesta por el artículo 33 RGPD, atendiendo a que la difusión de tales informaciones causaría un perjuicio claro a las funciones de investigación y sanción atribuidas a la AEPD y, adicionalmente, generaría un riesgo cierto de vulnerabilidad a los sistemas y procedimientos de seguridad implantados por los responsables del tratamiento. De ahí que, en estos casos, se haya avalado la aplicación de los límites establecidos en el artículo 14.1 LTAIBG hasta que concluya el procedimiento de control y se publique la correspondiente resolución.

   Sin embargo, la doctrina expuesta, cuyo mantenimiento se confirma, no resulta aplicable a este caso debido a que el objeto de la reclamación, tal y como se ha indicado, no es la información técnica y las demás circunstancias asociadas a una violación de la seguridad de datos personales, sino, únicamente, el dato relativo a *la fecha* en la que el responsable del tratamiento comunicó a la Autoridad de control una brecha de seguridad.

   A estos efectos, procede volver a recordar que la aplicación de los límites previstos en el artículo 14.1 LTAIBG debe partir necesariamente de que el derecho de acceso a la información pública es un derecho de rango constitucional que está reconocido y regulado en términos muy amplios en la propia Constitución y en la legislación de desarrollo, lo que obliga a interpretar de forma estricta, cuando no restrictiva, cualquier limitación que se pretenda imponer a su ejercicio, «*sin que quepa aceptar limitaciones que supongan un menoscabo injustificado y desproporcionado del derecho de acceso a la información*», tal como ha subrayado repetidamente el Tribunal Supremo (STS de 16 de octubre de 2017 - ECLI:ES:TS:2017:3530 y varias posteriores), requiriéndose en todo caso una «*justificación expresa y detallada que permita controlar la veracidad y proporcionalidad de la restricción establecida*» (STS de 11 de junio de 2020 - ECLI:ES:TS:2020:1558, entre otras).

   Como se ha señalado en múltiples ocasiones, el bien jurídico protegido por el límite previsto en el artículo 14.1.e) LTAIBG es la correcta tramitación y desarrollo de los procedimientos de investigación y sanción de carácter penal, administrativo o disciplinario, principalmente mientras estén siendo tramitados, de tal manera que la

R CTBG Número: 2026-0198 Fecha: 23/02/2026

investigación (y, en su caso, la correcta sanción de las infracciones o ilícitos cuya comisión quede acreditada) no se vea impedida por la divulgación de información. Por su parte, el bien jurídico protegido por el límite previsto en el artículo 14.1.g) LTAIBG es el de asegurar el correcto desenvolvimiento y el buen fin de la actividad de vigilancia, inspección y control realizada por las Administraciones Públicas —es decir, evitar que la divulgación de información sobre las estrategias, metodologías y operativas de investigación facilite eludir sanciones por infracciones efectivamente cometidas o dificulte detectar nuevas infracciones—.

En el presente caso, aun cuando así se afirma, no se justifica ni se alcanza a apreciar en qué medida la revelación de la concreta información sobre la fecha de comunicación de la brecha de seguridad podría perjudicar las actuaciones de investigación (y eventual sanción) emprendidas por la AEPD en relación con la violación de seguridad acaecida, o con el tratamiento posterior que el destinatario haya hecho de los datos personales revelados. En consecuencia, dada la exigencia de interpretación estricta y aplicación justificada y proporcionada a su objeto y finalidad de protección (artículo 14.2 LTAIBG), atendidas las circunstancias concurrentes, no cabe considerar justificada la aplicación de los límites del artículo 14.1 LTAIBG que han sido invocados.

7. Por otra parte, el organismo recurrido justifica la denegación del acceso parcial a la información previsto en el artículo 16 LTAIBG argumentando que del acceso al dato de la fecha de la notificación, sin el resto de la información, resultaría «*una información distorsionada y carente de sentido*»; y, en conexión con ello, sostiene que el interés público alegado por el recurrente para acceder a dicha información no puede reconducirse a ninguna de las finalidades de la LTAIBG.

   Para valorar debidamente estas alegaciones es pertinente traer a colación el tenor del artículo 33 RGPD, en cuyo apartado primero se establece lo siguiente:

   > «1. *En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.*»

   A la vista del contenido de este precepto, resulta evidente que el dato relativo a la fecha en la que un responsable del tratamiento notifica a la autoridad de control una

R CTBG Número: 2026-0198 Fecha: 23/02/2026

violación de la seguridad ocurrida en su organización no es una información *distorsionada o carente de sentido* si no está acompañada del resto de la información que, por imperativo del apartado tercero del mismo artículo 33 RGPD, debe incluirse en la notificación. Dado que el precepto establece un plazo de notificación, la fecha en la que ésta se produce posee un indudable sentido en sí misma, pues permite conocer si dicho plazo se ha observado.

Finalmente, tampoco cabe acoger la alegación referida a la inexistencia de un interés público conectado con las finalidades de la LTAIBG, dado que, al tratarse de una obligación impuesta por el RGPD a todos los responsables de tratamientos de datos personales, existe un indudable interés público en conocer el plazo el que la AEPD, en su condición de responsable del tratamiento, ha dado cumplimiento a esta obligación. En atención a ello, el acceso a la fecha solicitada entronca directamente con la finalidad que se destaca en el preámbulo de la LTAIBG de que la ciudadanía conozca «bajo qué criterios actúan nuestras instituciones».

8. Por las razones expuestas, se debe estimar la reclamación.

III. RESOLUCIÓN

En atención a los antecedentes y fundamentos jurídicos descritos, procede

PRIMERO: ESTIMAR la reclamación interpuesta frente a la resolución de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

SEGUNDO: INSTAR a la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS a que, en el plazo máximo de 10 días hábiles, remita al reclamante la siguiente información:

- *Fecha en la que comunicó la brecha de seguridad*

TERCERO: **INSTAR** a la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS a que, en el mismo plazo máximo, remita a este Consejo de Transparencia copia de la información enviada al reclamante.

De acuerdo con el artículo 23.1[7], de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, la reclamación prevista en el artículo 24 de la misma tiene la consideración de sustitutiva de los recursos administrativos, de

[7] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a23

R CTBG Número: 2026-0198 Fecha: 23/02/2026

conformidad con lo dispuesto en el artículo 112.2 de la Ley 39/2015, de 1 de octubre[8], de Procedimiento Administrativo Común de las Administraciones Públicas.

Contra la presente resolución, que pone fin a la vía administrativa, se podrá interponer recurso contencioso-administrativo, en el plazo de dos meses, directamente ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, de conformidad con lo previsto en el apartado quinto de la Disposición adicional cuarta de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-administrativa[9].

EL PRESIDENTE DEL CTBG

Fdo.: José Luis Rodríguez Álvarez

R CTBG
Número: 2026-0198 Fecha: 23/02/2026

[redacted]

[8] https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565&p=20151002&tn=1#a112
[9] https://www.boe.es/buscar/act.php?id=BOE-A-1998-16718&p=20230301&tn=1#dacuarta